AXIS I7010-VE Network Intercoms

AXIS I7010-VE Network Intercom
AXIS I7010-VE Safety Network Intercom

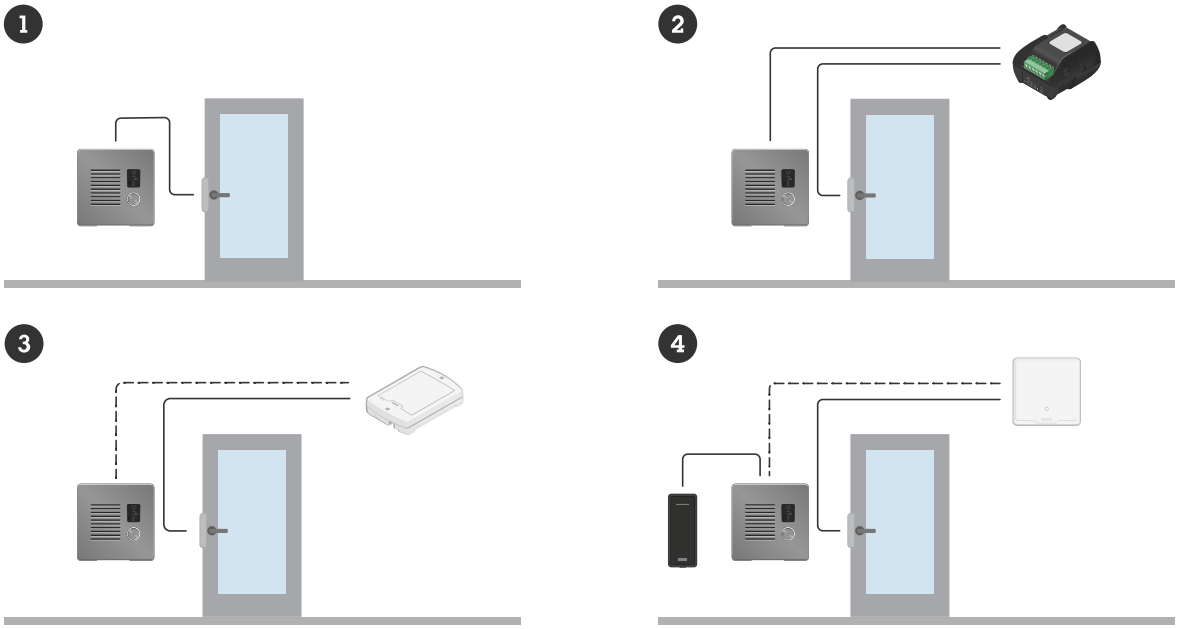
Manual do Usuário

Índice

Visão geral da configuração 4
Introdução 5
Encontre o dispositivo na rede 5
Suporte a navegadores 5
Abra a interface web do dispositivo 5
Crie uma conta de administrador 5
Senhas seguras 6
Certifique-se de que o software do dispositivo não foi manipulado 6
Configure seu dispositivo 7
Calibrar e executar um teste de alto-falante remoto 7
Configuração de SIP direto (P2P) 7
Configuração de SIP por meio de um servidor (PBX) 8
Incluir fluxo de vídeo da câmera próxima à chamada SIP 9
Criar um contato 9
Configurar o botão de chamada 9
Use DTMF para destravar a porta para um visitante 10
Use a lista de entradas para permitir que os detentores de credencial abram a porta 10
Configuração de regras de eventos 11
Acionar uma ação 11
A interface Web 12
Saiba mais 13
Voice over IP (VoIP) 13
Session Initiation Protocol (SIP) 13
SIP ponto a ponto (P2PSIP) 13
Private Branch Exchange (PBX) 14
NAT traversal 15
Analíticos e aplicativos 15
AXIS Client for Unified Communication Systems 15
Especificações 16
Visão geral do produto 16
Indicadores e controles do painel frontal 16
Ícones indicadores 16
Indicadores de LED 17
Slot de cartão SD 17
Botões 17
Botão de controle 17
Conectores 17
Conector de rede 17
Conector de áudio 17
Conector de E/S, leitor e relé 18
Conexão de equipamentos 20
Leitor Axis 20
Relé alimentado por PoE (12 V) 20
Relé alimentado por fonte separada 20
Relé sem potencial 21
Fechadura de 12 V protegida contra falhas alimentada via PoE pelo intercomunicador 21
Fechadura de 12 V protegida contra falhas alimentada por fonte externa 22
Solução de problemas 23
Restauração das configurações padrão de fábrica 23
Opções do AXIS OS 23
Verificar a versão atual do AXIS OS 23
Atualizar o AXIS OS 24
Problemas técnicos e possíveis soluções 24

Considerações sobre desempenho 26
Entre em contato com o suporte 27
Cibersegurança 28
Gerenciamento de vulnerabilidades 28
Notificações de segurança 28
Ciclo de vida seguro do produto 28
Informações de segurança 29
Níveis de perigo 29
Outros níveis de mensagens 29

Visão geral da configuração



1 *Intercomunicação*
2 *Intercomunicador combinado com a AXIS A9801*
3 *Intercomunicador combinado com a AXIS A9161*
4 *Interfone combinado com um leitor e um sistema de controle de acesso*

Introdução

Encontre o dispositivo na rede

Para encontrar dispositivos Axis na rede e atribuir endereços IP a eles no Windows®, use o AXIS IP Utility ou o AXIS Device Manager. Ambos os aplicativos são grátis e podem ser baixados de *axis.com/support*.

Para obter mais informações sobre como encontrar e atribuir endereços IP, acesse *Como atribuir um endereço IP e acessar seu dispositivo*.

Suporte a navegadores

O dispositivo pode ser usado com os seguintes navegadores:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Outros sistemas operacionais	*	*	*	*

✓: Recomendada

*: Compatível com limitações

Abra a interface web do dispositivo

1. Abra um navegador e digite o endereço IP ou o nome de host do dispositivo Axis.
   Se você não souber o endereço IP, use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede.
2. Digite o nome de usuário e a senha. Se você acessar o dispositivo pela primeira vez, você deverá criar uma conta de administrador. Consulte *Crie uma conta de administrador, on page 5*.

Para obter descrições de todos os recursos e configurações da interface Web dos dispositivos com AXIS OS, consulte *Ajuda da interface Web do AXIS OS*.

Crie uma conta de administrador

Na primeira vez que fizer login no dispositivo, você deverá criar uma conta de administrador.

1. Insira uma conta.
2. Insira uma senha. Consulte *Senhas seguras, on page 6*.
3. Insira a senha novamente.
4. Aceite o contrato de licença.
5. Clique em **Add account (Adicionar conta)**.

Importante

O dispositivo não possui conta padrão. Se você perder a senha da sua conta de administrador, deverá redefinir o dispositivo. Consulte *Restauração das configurações padrão de fábrica, on page 23*.

Senhas seguras

Importante

Use HTTPS (que vem ativado por padrão) para definir sua senha ou outras configurações confidenciais pela rede. HTTPS permite conexões de rede seguras e criptografadas, protegendo assim dados confidenciais, como senhas.

A senha do dispositivo é a proteção primária para seus dados e serviços. Os dispositivos Axis não impõem uma política de senhas, pois os produtos podem ser usados em vários tipos de instalações.

Para proteger seus dados, recomendamos enfaticamente que você:

- Use uma senha com pelo menos 8 caracteres, preferencialmente criada por um gerador de senhas.
- Não exponha a senha.
- Altere a senha em um intervalo recorrente pelo menos uma vez por ano.

Certifique-se de que o software do dispositivo não foi manipulado

Para certificar-se de que o dispositivo tenha o AXIS OS original ou para assumir o controle total do dispositivo após um ataque de segurança:

1. Restauração das configurações padrão de fábrica. Consulte *Restauração das configurações padrão de fábrica, on page 23*.
   Após a redefinição, uma inicialização segura garantirá o estado do dispositivo.
2. Configure e instale o dispositivo.

Configure seu dispositivo

Esta seção aborda todas as configurações importantes que um instalador precisa fazer para colocar o produto em funcionamento após a conclusão da instalação do hardware.

Calibrar e executar um teste de alto-falante remoto

É possível executar um teste de alto-falante para verificar remotamente se um alto-falante funciona conforme o planejado. O alto-falante executa o teste reproduzindo uma série de tons de teste registrados pelo microfone integrado. Toda vez que você executa o teste, os valores registrados são comparados aos valores que foram registrados durante a calibração.

Observação

O teste deve ser calibrado a partir de sua posição montada no local de instalação. Se o alto-falante for movido ou se o ambiente local mudar, por exemplo, se uma parede for construída ou removida, o alto-falante deverá ser calibrado novamente

Durante a calibração, recomenda-se que alguém permaneça fisicamente presente no local da instalação para ouvir os tons de teste e garantir que eles não estejam sendo abafados ou bloqueados por quaisquer obstruções não intencionais no caminho acústico do alto-falante.

1. Vá para a interface do dispositivo > **Audio > Speaker test (Áudio > Teste de alto-falante)**.
2. Para calibrar o dispositivo de áudio, clique em **Calibrate (Calibrar)**.

Observação

Após o produto Axis ser calibrado, o teste de alto-falante poderá ser executado a qualquer momento.

3. Para executar o teste de alto-falante, clique em **Run the test (Executar o teste)**.

Observação

Também é possível executar a calibração pressionando o botão de controle no dispositivo físico. Consulte *Visão geral do produto, on page 16* para identificar o botão de controle.

Configuração de SIP direto (P2P)

VoIP (Voice over IP) é um grupo de tecnologias que permite a comunicação por voz e multimídia via redes IP. Para obter mais informações, consulte *Voice over IP (VoIP), on page 13*.

Neste dispositivo, o VoIP é habilitado pelo protocolo SIP. Para obter mais informações sobre SIP, consulte *Session Initiation Protocol (SIP), on page 13*.

Há dois tipos de configurações para o SIP. Direto ou ponto a ponto (P2P) é um deles. Use ponto a ponto quando a comunicação for feita entre alguns agentes de usuário na mesma rede IP e não houver necessidade de recursos adicionais que poderiam ser fornecidos por um servidor PBX. Para obter informações sobre como configurar esse tipo de comunicação, consulte *SIP ponto a ponto (P2PSIP), on page 13*.

1. Vá para **Communication > SIP > Settings (Comunicação > SIP > Configurações de SIP)** e selecione **Enable SIP (Habilitar SIP)**.
2. Para permitir que o dispositivo receba chamadas, selecione **Allow incoming calls (Permitir recebimento de chamadas)**.

OBSERVAÇÃO

Quando você permite o recebimento de chamadas, o dispositivo aceita chamadas de qualquer dispositivo conectado à rede. Se o dispositivo puder ser acessado de uma rede pública ou pela Internet, recomendamos não permitir o recebimento de chamadas.

3. Clique em **Call handling (Tratamento de chamadas)**.
4. Em **Calling timeout (Tempo limite de chamada)**, defina por quantos segundos a chamada irá durar se não houver resposta.
5. Se você tiver permitido o recebimento de chamadas defina o número de segundos antes da espera de chamadas de entrada no **Incoming call timeout (Tempo limite de recebimento de chamadas)**.

6. Clique em **Ports (Portas)**.
7. Insira o número da **SIP port (Porta SIP)** e o número da **TLS port (Porta TLS)**.

Observação

- **SIP port (Porta SIP)** – Para sessões de SIP. O tráfego de sinalização por essa porta não é criptografado. O número da porta padrão é 5060.
- **TLS port (Porta TLS)** – Para sessões de SIP protegidas por SIPS e TLS. O tráfego de sinalização por meio dessa porta é criptografado com o Transport Layer Security (TLS). O número da porta padrão é 5061.
- **RTP start port (Porta de início de RTP)** – a porta usada para o primeiro stream de mídia RTP em uma chamada SIP. A porta padrão inicial é 4000. Alguns firewalls podem bloquear o tráfego RTP em determinados números de porta. O número da porta deve ser entre 1024 e 65535.

8. Clique em **NAT traversal**.
9. Selecione os protocolos que deseja ativar para o NAT traversal.

Observação

Use o NAT traversal quando o dispositivo estiver conectado à rede por trás de um roteador NAT ou um firewall. Para obter mais informações consulte *NAT traversal, on page 15*.

10. Clique em **Save (Salvar)**.

Configuração de SIP por meio de um servidor (PBX)

VoIP (Voice over IP) é um grupo de tecnologias que permite a comunicação por voz e multimídia via redes IP. Para obter mais informações, consulte *Voice over IP (VoIP), on page 13*.

Neste dispositivo, o VoIP é habilitado pelo protocolo SIP. Para obter mais informações sobre SIP, consulte *Session Initiation Protocol (SIP), on page 13*.

Há dois tipos de configurações para o SIP. Um servidor PBX é um deles. Use um servidor PBX quando a comunicação precisar ser feita entre um número infinito de agentes de usuário dentro e fora da rede IP. Recursos adicionais podem ser adicionados à configuração dependendo do provedor de PBX. Para obter mais informações, consulte *Private Branch Exchange (PBX), on page 14*.

1. Solicite as seguintes informações do seu provedor de PBX:
   - ID de usuário
   - Domínio
   - Senha
   - ID de autenticação
   - ID do chamador
   - Registrador
   - Porta de início de RTP
2. Acesse **Communication > SIP > Accounts (Comunicação > SIP > Contas)** e clique em **+ Add account (+ Adicionar conta)**.
3. Insira um **Name (Nome)** para a conta.
4. Selecione **Registered (Registrado)**.
5. Selecione um modo de transporte.
6. Adicione as informações da conta a partir do provedor de PBX.
7. Clique em **Save (Salvar)**.
8. Defina as configurações de SIP da mesma forma que para ponto a ponto, consulte *Configuração de SIP direto (P2P), on page 7*. Use a porta de início de RTP do provedor de PBX.

Incluir fluxo de vídeo da câmera próxima à chamada SIP

Se você tiver uma câmera Axis instalada perto do intercomunicador, poderá incluir o fluxo de vídeo da câmera em suas chamadas SIP e VMS do intercomunicador.

Requisitos

Uma câmera Axis com H.264 e resolução de 1280x720, 800x800 ou 640x480.

Para conectar o interfone à câmera:

1. Vá para **System > Edge-to-edge > Pairing (Sistema > Edge-to-edge > Pareamento)**.
2. Em **Emparelhamento de câmeras**, digite o endereço, o nome de usuário e a senha da câmera Axis.
3. Clique em **Conectar**.

Criar um contato

Este exemplo explica como criar um novo contato na lista de contatos. Antes de iniciar, ative o SIP em **Communication > SIP (Comunicação > SIP)**.

Para criar um novo contato:

1. Vá para **Communication > Contact list (Comunicação > Lista de contatos)**.
2. Clique em **+ Add contact (+ Adicionar contato)**.
3. Insira o nome e o sobrenome do contato.
4. Insira o endereço SIP do contato.

Observação

Para obter informações sobre os endereços SIP, consulte *Session Initiation Protocol (SIP), on page 13*.

5. Selecione a conta SIP da qual a chamada será efetuada.

Observação

As opções de disponibilidade são definidas em **System (Sistema)** > **Events (Eventos)** > **Schedules (Agendamentos)**.

6. Escolha a **Availability (Disponibilidade)** do contato. Se houver uma chamada quando o contato não estiver disponível, a chamada é cancelada, a menos que haja um contato de fallback.

Observação

Um fallback é um contato para quem a chamada é encaminhada se o contato original não responde ou fica indisponível.

7. Em **Fallback**, selecione **Nenhum**.
8. Clique em **Save (Salvar)**.

Configurar o botão de chamada

Por padrão, o botão de chamada é configurado para fazer chamadas de VMS (sistema de gerenciamento de vídeo). Se você desejar manter essa configuração, basta adicionar o intercomunicador Axis ao VMS.

Este exemplo explica como configurar o sistema para ligar para um contato da lista de contatos quando um visitante pressionar o botão de chamada.

1. Acesse **Communication > Calls > Call button (Comunicação > Chamadas > Botão de chamadas)**.
2. Em **Recipients (Destinatários)**, remova **VMS**.
3. Em **Recipients (Destinatários)**, selecione um existente ou crie um contato.

Para desativar o botão de chamada, desative **Enable call button (Ativar botão de chamada)**.

Use DTMF para destravar a porta para um visitante

Quando um visitante faz uma chamada no intercomunicador, a pessoa que responde pode usar sinalização Dual-Tone Multi-Frequency (DTMF) do seu dispositivo SIP para destravar a porta. O controlador de porta destrava e trava a porta.

Este exemplo explica como:

- definir o sinal DTMF no intercomunicador
- configurar o intercomunicador para:
  - solicitar ao controlador de porta o destravamento da porta **ou**
  - destravar a porta usando o relé interno.

Todas as configurações são ajustadas na página da Web do intercomunicador.

Antes de começar

- Permita chamadas SIP do dispositivo e crie uma conta SIP. Consulte *Configuração de SIP direto (P2P), on page 7* e *Configuração de SIP por meio de um servidor (PBX), on page 8*.

Defina o sinal DTMF no intercomunicador

1. Acesse **Communication > SIP > DTMF (Comunicação > SIP > DTMF)**.
2. Clique em **+ Add sequence (+ Adicionar sequência)**.
3. Em **Sequence (Sequência)**, insira 1.
4. Em **Descrição**, insira Destravar porta.
5. Em **Accounts (Contas)**, selecione a conta SIP.
6. Clique em **Save (Salvar)**.

Configure o intercomunicador para destravar a porta usando o relé interno

7. Acesse **System > Events > Rules (Sistema > Eventos > Regras)** e adicione uma regra:
8. No campo **Nome**, insira DTMF Destravar porta.
9. Na lista de condições, em **Call (Chamada)**, selecione **DTMF** e **Unlock door (Destravar porta)**.
10. Na lista de ações, em **I/O (E/S)**, selecione **Toggle I/O once (Alternar E/S uma vez)**.
11. Na lista de portas, selecione **Relay 1 (Relé 1)**.
12. Altere **Duration (Duração)** para 00:00:07, o que significa que a porta está aberta por 7 segundos.
13. Clique em **Save (Salvar)**.

Use a lista de entradas para permitir que os detentores de credencial abram a porta

Com a lista de entradas, você pode possibilitar que os detentores de credenciais usem sua credencial para acionar ações, como abrir uma porta. Este exemplo explica como adicionar um detentor de credencial que pode usar o cartão para abrir a porta dez vezes.

Pré-requisitos

- O tipo de chip correto deve estar ativo em **Reader > Chip types (Leitor > Tipos de chip)**.

Ative a lista de entradas e adicione um detentor de credencial:

1. Acesse **Reader > Entry list (Leitor > Lista de entrada)**.
2. Ative a opção **Use Entry list (Usar lista de entrada)**.
3. Clique em **+ Add credential holder (+ Adicionar detentor de credencial)**.
4. Digite o nome e o sobrenome do detentor da credencial. O primeiro nome deve ser único.
5. Selecione **Card (Cartão)**.
6. Passe o cartão do detentor de credencial no dispositivo e clique em **Get latest (Obter mais recente)**.
7. Mantenha a condição do evento como **Access granted (Acesso concedido)**.

8. Em **Valid to (Válido até)**, selecione **Number of times (Número de vezes)**.
9. Em **Número de vezes**, insira 10.
10. Clique em **Save (Salvar)**.

Crie uma regra:

1. Acesse **System > Events (Sistema > Eventos)**.
2. Em **Rules (Regras)**, clique em **+Add a rule (+ Adicionar regra)**.
3. Em **Nome**, digite Abrir porta.
4. Na lista de condições, selecione **Entry list > Access granted (Lista de entrada > Acesso concedido)**.
5. Na lista de ações, selecione **I/O > Toggle I/O once (E/S > Alternar E/S uma vez)**.
6. Na lista de portas, selecione **Door (Porta)**.
7. Em **State (Estado)**, selecione **Active (Ativo)**.
8. Defina a duração para 00:00:07.
9. Clique em **Save (Salvar)**.

Configuração de regras de eventos

Você pode criar regras para fazer com que o dispositivo realize ações quando certos eventos ocorrem. Uma regra consiste em condições e ações. As condições podem ser usadas para acionar as ações. Por exemplo, o dispositivo pode iniciar uma gravação ou enviar um email quando detecta movimento ou mostrar um texto de sobreposição enquanto o dispositivo está gravando.

Para saber mais, consulte *Comece a utilizar regras para eventos*.

Acionar uma ação

1. Vá para **System (Sistema)** > **Events (Eventos)** e clique em **+ Add a rule (+Adicionar uma regra)**. A regra define quando o dispositivo executará determinadas ações. Você pode configurar regras como agendadas, recorrentes ou acionadas manualmente.
2. Insira um **Name (Nome)**.
3. Selecione a **Condition (Condição)** que deve ser atendida para acionar a ação. Se você especificar mais de uma condição para a regra, todas as condições deverão ser atendidas para acionar a ação.
4. Selecione qual **Ação** executar quando as condições forem atendidas.

A interface Web

Para saber mais sobre todos os recursos e configurações disponíveis na interface Web dos dispositivos com AXIS OS, vá para *Ajuda da interface Web do AXIS OS*.

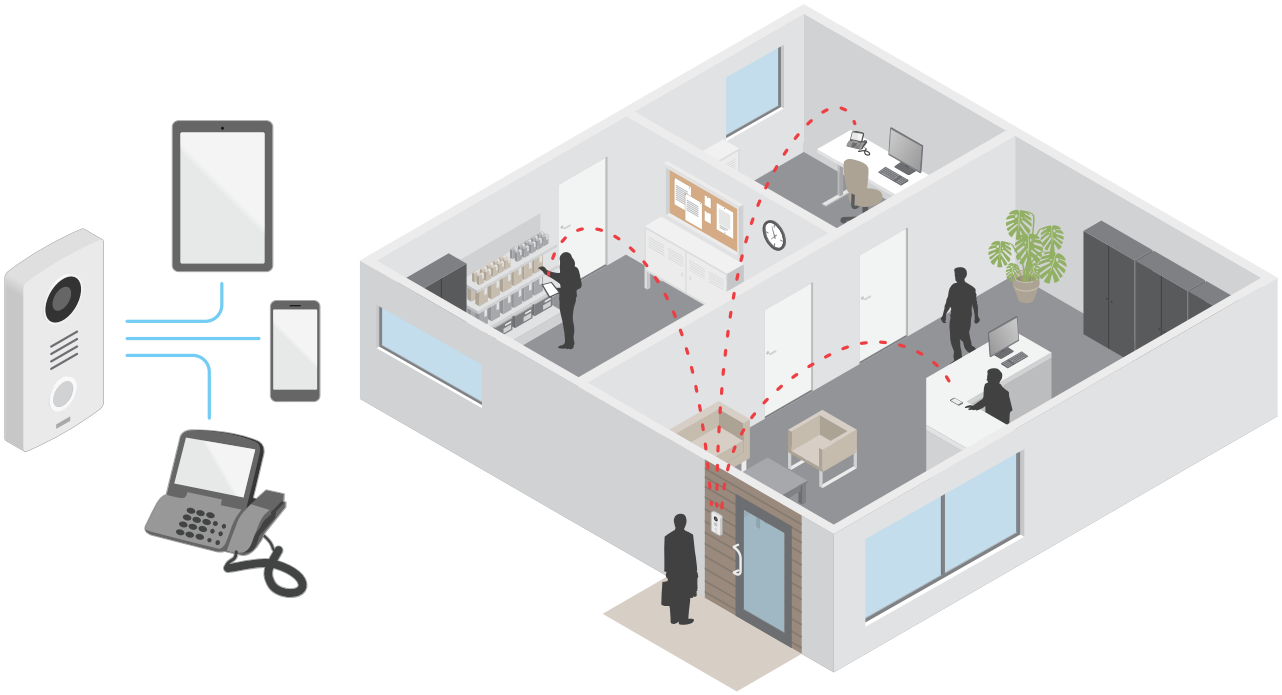
Saiba mais

Voice over IP (VoIP)

Voice over IP (VoIP) é um grupo de tecnologias que permite a comunicação por voz e sessões multimídia via redes IP, como a Internet. Em chamadas telefônicas tradicionais, os sinais analógicos são enviados através de transmissões de circuito através da rede de telefonia comutada pública (PSTN). Em uma chamada VoIP, os sinais analógicos são convertidos em sinais digitais para possibilitar o envio de pacotes de dados via redes IP locais ou pela Internet.

No produto Axis, o VoIP é possibilitado pelo Session Initiation Protocol (SIP) e a sinalização Dual-Tone multi--Frequency (DTMF).

Exemplo:



Quando você pressiona o botão de chamada em um intercomunicador Axis, uma chamada é iniciada para um ou mais destinatários predefinidos. Quando um destinatário responde, uma chamada é estabelecida. A voz e o vídeo são transmitidos por meio de tecnologias VoIP.

Session Initiation Protocol (SIP)

O Session Initiation Protocol (SIP) é usado para configurar, manter e encerrar chamadas de VoIP. Você pode fazer chamadas entre duas ou mais partes, chamadas de agentes de usuário SIP. Para fazer uma chamada SIP, você pode usar, por exemplo, telefones SIP, softphones ou dispositivos Axis compatíveis com SIP.

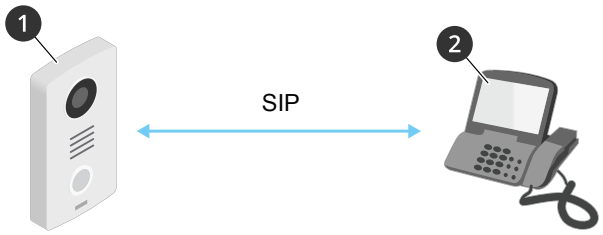
O áudio ou vídeo efetivos são trocados entre os agentes de usuário SIP com um protocolo de transporte, por exemplo, RTP (Real-Time Transport Protocol).

Você pode fazer chamadas em redes locais usando uma configuração ponto a ponto ou através de redes que usam um PBX.

SIP ponto a ponto (P2PSIP)

O tipo mais básico de comunicação SIP ocorre diretamente entre dois ou mais agentes de usuário SIP. Isso é chamado de SIP ponto a ponto (P2PSIP). Se ele ocorre em uma rede local, tudo o que é necessário são os endereços SIP dos agentes de usuário. Um endereço SIP típico, nesse caso, seria `sip:<local-ip>`.

Exemplo:



1 *Agente de usuário A – intercomunicador. Endereço SIP: sip:192.168.1.101*
2 *Agente de usuário B – telefone compatível com SIP. Endereço SIP: sip:192.168.1.100*

Você pode configurar o intercomunicador Axis para chamar, por exemplo, um telefone compatível com SIP na mesma rede usando uma configuração de SIP ponto a ponto.

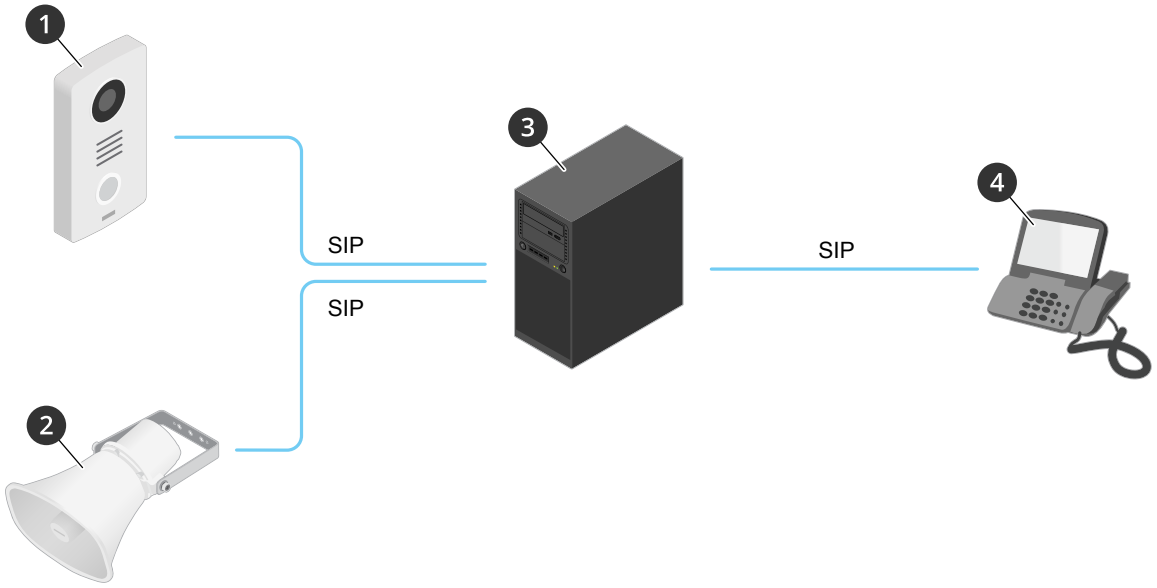
Private Branch Exchange (PBX)

Quando você faz chamadas SIP fora da sua rede IP local, um PBX (Private Branch Exchange) pode atuar como hub central. O componente principal de um PBX é um servidor SIP, o qual também é conhecido como proxy SIP ou registrador. Um PBX funciona como uma mesa telefônica tradicional, mostrando o status atual do cliente e permitindo transferências de chamadas, correio de voz e redirecionamentos.

O servidor SIP de PBX pode ser configurado como uma entidade local ou externa. Ele pode ser hospedado em uma intranet ou por um provedor terceirizado. Quando você faz chamadas SIP entre redes, as chamadas são roteadas através de um conjunto de PBXs, que consultam o local do endereço SIP a ser acessado.

Cada agente de usuário SIP registra-se no PBX e pode, em seguida, alcançar os outros discando o ramal correto. Um endereço IP típico nesse caso seria `sip:<user>@<domain>` ou `sip:<user>@<registrar-ip>`. O endereço SIP é independente de seu endereço IP e o PBX torna o dispositivo acessível, desde que esteja registrado no PBX.

Exemplo:



1 *sip:minhaporta@empresa.com*
2 *sip:meualtofalante@empresa.com*
3 ***PBX** sip.empresa.com*
4 *sip:escritório@empresa.com*

Quando você pressiona o botão de chamada em um intercomunicador Axis, a chamada é encaminhada através de um ou mais PBXs para um endereço SIP na rede IP local ou via Internet.

NAT traversal

Use o NAT (Network Address Translation) traversal quando o dispositivo Axis estiver localizado em uma rede privada (LAN) e você deseja acessá-lo de fora dessa rede.

Observação

O roteador deve ser compatível com o NAT traversal e UPnP®.

Cada protocolo de NAT traversal pode ser usado separadamente ou em diferentes combinações, dependendo do ambiente de rede.

- **ICE** – O protocolo ICE (Interactive Connectivity Establishment) aumenta as chances de encontrar o caminho mais eficiente para uma comunicação bem-sucedida entre dispositivos. Se você também ativar o STUN e o TURN, poderá melhorar as chances do protocolo ICE.
- **STUN** – O STUN (Session Traversal Utilities for NAT) é um protocolo de rede cliente-servidor que permite que o dispositivo Axis determine se ele está localizado atrás de um NAT ou firewall e, em caso afirmativo, obtenha o endereço IP público mapeado e o número da porta alocada para conexões a hosts remotos. Insira o endereço do servidor STUN, por exemplo, um endereço IP.
- **TURN** – O TURN (Traversal Using Relays around NAT) é um protocolo que permite que um dispositivo atrás de um roteador NAT ou firewall receba dados de outros hosts via TCP ou UDP. Insira o endereço do servidor TURN e as informações de login.

Analíticos e aplicativos

Usando analíticos e aplicativos, você pode obter mais do seu dispositivo Axis. O AXIS Camera Application Platform (ACAP) é uma plataforma aberta que permite que qualquer pessoa desenvolva analíticos e outros aplicativos para dispositivos Axis. Os aplicativos podem ser pré-instalados no dispositivo, disponibilizados para download gratuitamente ou mediante uma taxa de licença.

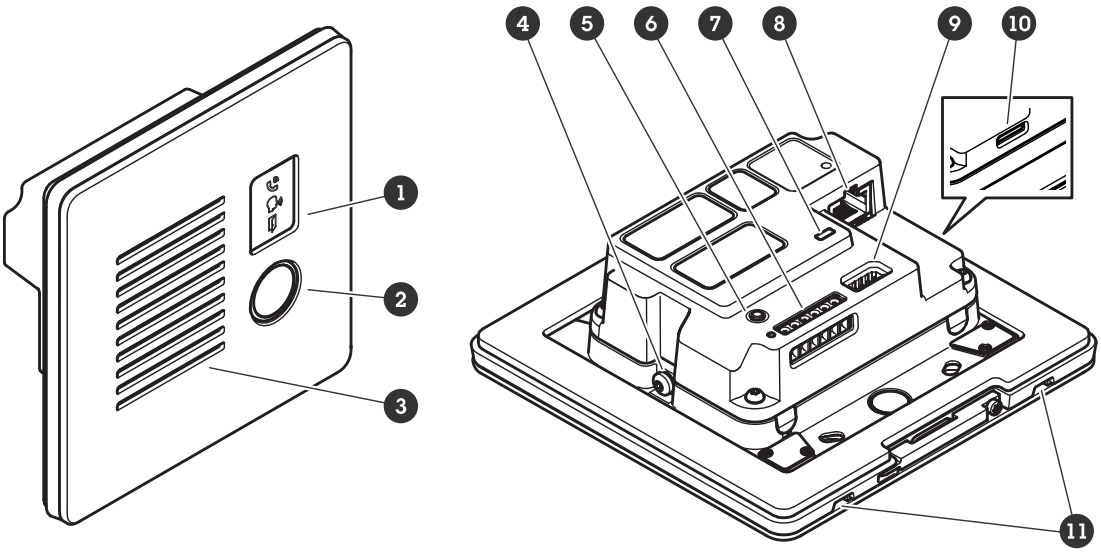
Para encontrar manuais de usuário de analíticos e aplicativos da Axis, vá para *help.axis.com*.

AXIS Client for Unified Communication Systems

Com este aplicativo, você pode fazer chamadas entre dispositivos Axis habilitados para SIP e contas vinculadas do Microsoft® Teams. Para obter mais informações, consulte o *manual do usuário do AXIS Client for Unified Communication Systems*.

Especificações

Visão geral do produto



1 *Ícones indicadores, on page 16*
2 *Botão de chamada*
3 *Alto-falante*
4 *Parafuso de aterramento*
5 *Botão de controle, on page 17*
6 *Conector de E/S, leitor e relé, on page 18*
7 *LED de estado*
8 *Conector de rede, on page 17*
9 *Conector de áudio, on page 17*
10 *Slot de cartão SD, on page 17 (microSD/microSDHC/microSDXC)*
11 *Microfone (x 2)*

Indicadores e controles do painel frontal

Quando você conecta o produto a alimentação, os indicadores do painel frontal se acendem por alguns segundos.

Ícones indicadores

Ícone	Indicação
	Aceso em âmbar quando a chamada enviada é iniciada. Pisca em âmbar quando a chamada recebida é iniciada.
	Aceso em azul para chamada em andamento.
	Aceso em verde quando a porta está aberta.

Indicadores de LED

LED de estado	Indicação
Verde	Aceso em verde para operação normal.

Slot de cartão SD

OBSERVAÇÃO

- Risco de danos ao cartão SD. Não utilize ferramentas afiadas, objetos metálicos nem force excessivamente ao inserir ou remover o cartão SD. Use os dedos para inserir e remover o cartão.
- Risco de perda de dados ou gravações corrompidas. Desmonte o cartão SD pela interface web do dispositivo antes de removê-lo. Não remova o cartão SD com o produto em funcionamento.

Esse dispositivo é compatível com cartões microSD/microSDHC/microSDXC.

Para obter recomendações sobre cartões SD, consulte *axis.com*.

Os logotipos microSD, microSDHC e microSDXC são marcas comerciais da SD-3C LLC. microSD, microSDHC e microSDXC são marcas comerciais ou registradas da SD-3C, LLC nos Estados Unidos e/ou em outros países.

Botões

Botão de controle

O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte *Restauração das configurações padrão de fábrica, on page 23*.
- Conexão a um serviço de conexão em nuvem com um clique (O3C) via Internet. Para conectar, pressione e solte o botão e aguarde até que o LED de status pisque em verde três vezes.

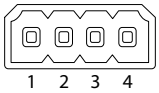
Conectores

Conector de rede

Conector Ethernet RJ45 com Power over Ethernet (PoE).

Conector de áudio

Bloco de terminais com 4 pinos para entrada e saída de áudio.

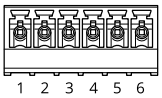


Função	Pin	Observações
Entrada de linha	1	Entrada de áudio (mono)
GND	2	Aterramento de áudio
Saída de linha	3	Saída de áudio (mono)
GND	4	Aterramento de áudio

Conector de E/S, leitor e relé

Esse conector pode ser usado para E/S e relé ou para conectividade do leitor.

Bloco terminal com 6 pinos



1 -
2 *12 V*
3 *A/IO1*
4 *B/IO2*
5 *COM*
6 *NO/NC*

Função	Pin	Observações	Especificações
Terra CC	1		0 VCC
Saída CC	2	Pode ser usado para alimentar equipamentos auxiliares se o dispositivo for alimentado por classe 4 de PoE. Observação: esse pino pode ser usado somente como saída de energia.	12 V CC **E/S** : Carga máxima = 50 mA **Leitor/relé**: Carga máxima = 350 mA
I/O (E/S): Configurável (entrada ou saída) **Leitor**: A	3	**I/O (E/S)**: Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar. Saída digital – Conectado internamente ao pino 1 (terra CC) quando ativo, flutuante (desconectado) quando inativo. Se usada com uma carga indutiva (por exemplo, um relé), conecte um diodo em paralelo à carga para proporcionar proteção contra transientes de tensão. **Leitor**: RS485 – A	**E/S** : entrada – 0 a máx. 30 V DC saída – 0 a máx. 30 V DC, dreno aberto, 100 mA
I/O (E/S): Configuraável (entrada ou saída) **Leitor**: B	4	**I/O (E/S)**: o mesmo que o pino 3 **Leitor**: RS485 – B	**I/O (E/S)**: o mesmo que o pino 3
Relé: COM	5	Comum	
Relé: NO/NC	6	Normalmente aberto/Normalmente fechado. Para conectar dispositivos de relé. Os dois pinos de relé estão galvanicamente separados do resto do circuito.	Corrente máx. = 700 mA, tensão máx. = 30 VCC

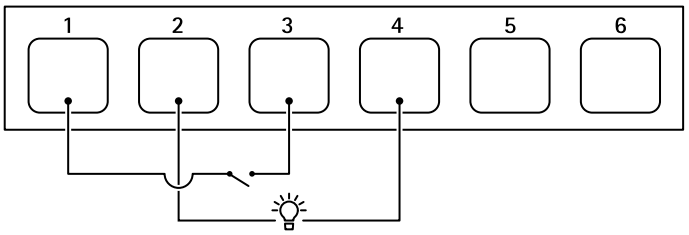
Conector de E/S

Uma opção é usar o conector como um conector de E/S com dispositivos externos em combinação com, por exemplo, detectores de movimento, acionadores de eventos e notificações de alarmes. Além do ponto de referência de 0 VCC e da alimentação (saída CC de 12 V), o conector do terminal de E/S fornece a interface para:

Entrada digital – Para conectar dispositivos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas/janelas e detectores de quebra de vidros.

Saída digital – Para conectar dispositivos externos, como relés e LEDs. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativos VAPIX®, por meio de um evento ou via interface do dispositivo.

Exemplo:



1 *Terra CC*
2 *Saída CC 12 V, máx. 50 mA*
3 *E/S configurada como entrada*
4 *E/S configurada como saída*
5 *Somente relé*
6 *Somente relé*

Conector do relé

Em combinação com a E/S, você pode usar o conector como conector de relé para conectar um relé de estado sólido e usá-lo:

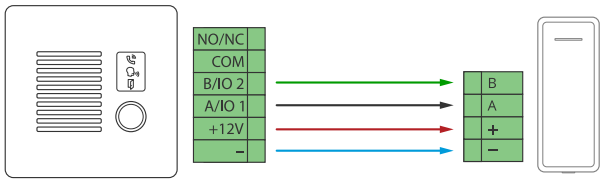
- como um relé padrão que abre e fecha circuitos auxiliares,
- para controlar diretamente uma fechadura,
- para controlar uma trava por meio de um relé de segurança. Usar um relé de segurança no lado seguro da porta evita hotwiring.

Conector do leitor

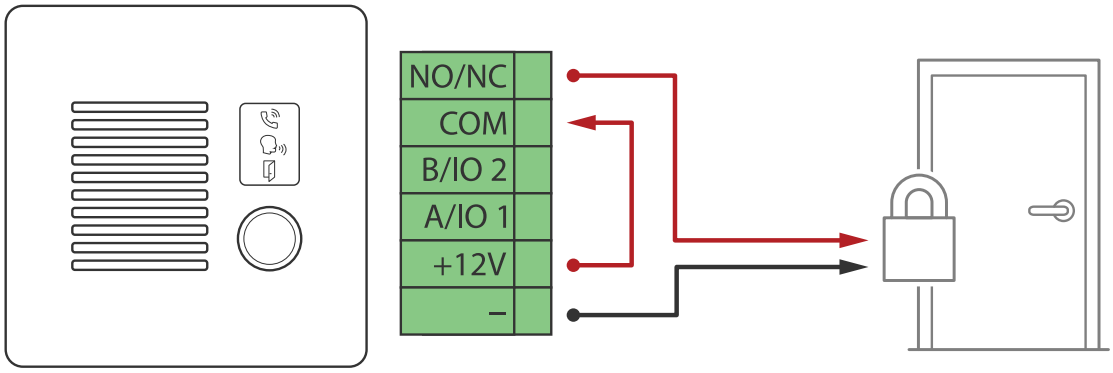
Uma terceira opção é usar o conector como conector de leitor para conectar um leitor externo.

Conexão de equipamentos

Leitor Axis

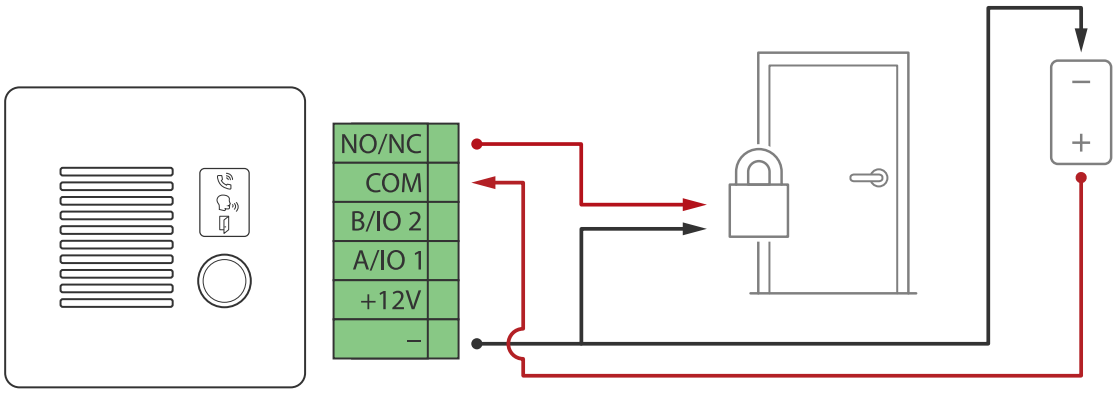


Relé alimentado por PoE (12 V)



1. Para verificar o estado do relé, vá para **System > Accessories (Sistema > Acessórios)** e encontre a porta do relé.
2. Defina **Normal state (Estado normal)** como:
   - para uma fechadura protegida contra falhas.
   - para uma fechadura protegida contra falhas.

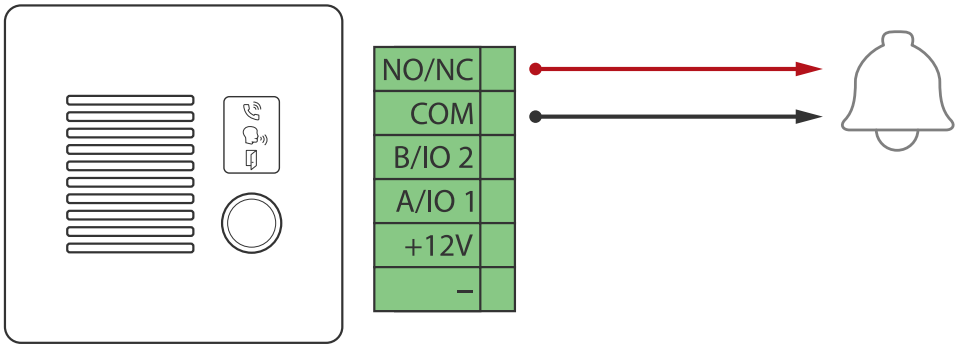
Relé alimentado por fonte separada



1. Para verificar o estado do relé, vá para **System > Accessories (Sistema > Acessórios)** e encontre a porta do relé.
2. Defina **Normal state (Estado normal)** como:
   - para uma fechadura protegida contra falhas.

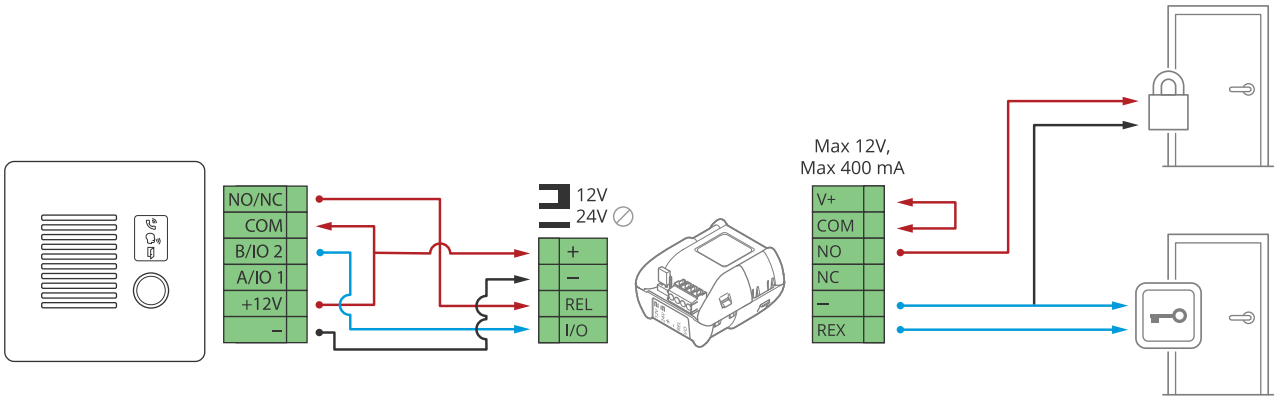
– para uma fechadura protegida contra falhas.

Relé sem potencial



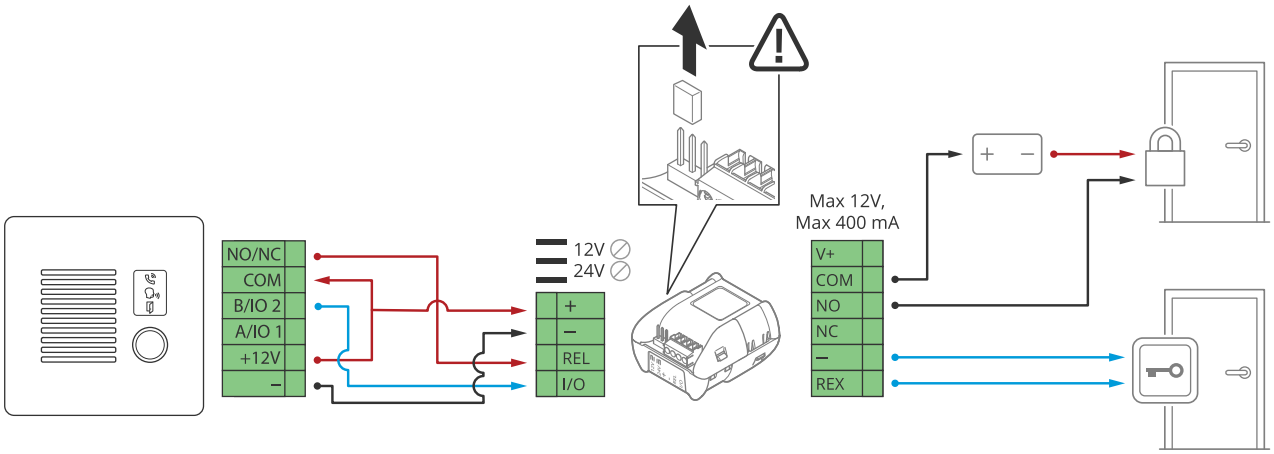
1. Para verificar o estado do relé, vá para **System > Accessories (Sistema > Acessórios)** e encontre a porta do relé.
2. Defina **Normal state (Estado normal)** como:
   – para uma fechadura protegida contra falhas.
   – para uma fechadura protegida contra falhas.

Fechadura de 12 V protegida contra falhas alimentada via PoE pelo intercomunicador



1. Para verificar o estado do relé, vá para **System > Accessories (Sistema > Acessórios)** e encontre a porta do relé.
2. Defina **Normal state (Estado normal)** como:
   – para uma fechadura protegida contra falhas.
   – para uma fechadura protegida contra falhas.

Fechadura de 12 V protegida contra falhas alimentada por fonte externa



1. Para verificar o estado do relé, vá para **System > Accessories (Sistema > Acessórios)** e encontre a porta do relé.
2. Defina **Normal state (Estado normal)** como:
   -  para uma fechadura protegida contra falhas.
   -  para uma fechadura protegida contra falhas.

Solução de problemas

Restauração das configurações padrão de fábrica

Importante

A restauração para as configurações padrão de fábrica deve ser feita com muito cuidado. Uma redefinição para os padrões de fábrica restaura todas as configurações, inclusive o endereço IP, para os valores padrão de fábrica.

Para redefinir o produto para as configurações padrão de fábrica:

1. Desconecte a alimentação do produto.
2. Mantenha o botão de controle pressionado enquanto reconecta a alimentação. Consulte *Visão geral do produto, on page 16*.
3. Mantenha o botão de controle pressionado por cerca de 15 a 30 segundos até que o indicador do LED de estado pisque com a cor âmbar.
4. Solte o botão de controle. O processo estará concluído quando o indicador do LED de estado ficar verde. Se nenhum servidor DHCP estiver disponível na rede, o endereço IP do dispositivo será padrão para um dos seguintes:
   - **Dispositivos com AXIS OS 12.0 e versões posteriores:** Obtidos da sub-rede de endereço local do link (169.254.0.0/16)
   - **Dispositivos com AXIS SO 11.11 e anterior:** 192.168.0.90/24
5. Use as ferramentas de software de instalação e gerenciamento para atribuir um endereço IP, definir a senha e acessar o dispositivo.
   As ferramentas de software de instalação e gerenciamento estão disponíveis nas páginas de suporte em *axis.com/support*.

Você também pode redefinir os parâmetros para as configurações padrão de fábrica na interface Web do dispositivo. Vá para **Maintenance (Manutenção)** > **Factory default (Padrão de fábrica)** e clique em **Default (Padrão)**.

Opções do AXIS OS

A Axis oferece o gerenciamento de software de dispositivo de acordo com a trilha ativa ou com as trilhas de suporte de longo prazo (LTS). Estar na trilha ativa significa que você obtém acesso contínuo a todos os recursos de produtos mais recentes, enquanto as trilhas de LTS fornecem uma plataforma fixa com versões periódicas voltadas principalmente para correções de erros e atualizações de segurança.

Usar os AXIS OS da trilha ativa é recomendado se você deseja acessar os recursos mais recentes ou se você usa as ofertas de sistema ponta a ponta Axis. As trilhas de LTS são recomendados se você usa integrações de outros fabricantes, as quais podem não ser continuamente validadas com a trilha ativa mais recente. Com o LTS, os produtos podem manter a segurança cibernética sem apresentar quaisquer alterações funcionais significativas nem afetar quaisquer integrações existentes. Para obter informações mais detalhadas sobre a estratégia de software de dispositivos Axis, acesse *axis.com/support/device-software*.

Verificar a versão atual do AXIS OS

O AXIS OS determina a funcionalidade de nossos dispositivos. Durante o processo de solução de um problema, recomendamos que você comece conferindo a versão atual do AXIS OS. A versão mais recente pode conter uma correção que soluciona seu problema específico.

Para verificar a versão atual do AXIS OS:

1. Vá para a interface Web do dispositivo > **Status**.
2. Em **Device info (Informações do dispositivo)**, consulte a versão do AXIS OS.

Atualizar o AXIS OS

Importante

- Ao atualizar o software do dispositivo, suas configurações pré-definidas e personalizadas serão salvas. A Axis Communications AB não pode garantir que as configurações sejam salvas, mesmo que os recursos estejam disponíveis na nova versão do AXIS OS.
- A partir do AXIS OS 12.6, é necessário instalar todas as versões LTS entre a versão atual do seu dispositivo e a versão de destino. Por exemplo, se a versão atualmente instalado do software for AXIS OS 11.2, você terá que instalar a versão LTS AXIS OS 11.11 antes de poder fazer o upgrade do dispositivo para AXIS OS 12.6. Para obter mais informações, consulte *Guia do ciclo de vida do AXIS OS: Caminho de atualização*.
- Certifique-se de que o dispositivo permaneça conectado à fonte de alimentação ao longo de todo o processo de atualização.

Observação

- Quando você atualiza o dispositivo com a versão mais recente do AXIS OS na trilha ativa, o produto recebe a última funcionalidade disponível. Sempre leia as instruções de atualização e notas de versão disponíveis com cada nova versão antes de atualizar. Para encontrar a versão do AXIS OS e as notas de versão mais recentes, vá para *axis.com/support/device-software*.

1. Baixe o arquivo do AXIS OS para seu computador, o qual está disponível gratuitamente em *axis.com/ /support/device-software*.
2. Faça login no dispositivo como um administrador.
3. Vá para **Maintenance (Manutenção) > AXIS OS upgrade (Atualização do AXIS OS)** e clique em **Upgrade (Atualizar)**.

Após a conclusão da atualização, o produto será reiniciado automaticamente.

Problemas técnicos e possíveis soluções

Problemas ao atualizar o AXIS OS

A atualização do AXIS OS falhou

Se a atualização falhar, o dispositivo recarregará a versão anterior. O motivo mais comum é que o arquivo de incorreto do AXIS OS foi carregado. Verifique se o nome do arquivo do AXIS OS corresponde ao seu dispositivo e tente novamente.

Problemas após a atualização do AXIS OS

Se você tiver problemas após a atualização, reverta para a versão instalada anteriormente na página **Maintenance (Manutenção)**.

Problemas na configuração do endereço IP

Não é possível definir o endereço IP

- Se o endereço IP destinado ao dispositivo e o endereço IP do computador usado para acessar o dispositivo estiverem localizados em sub-redes diferentes, você não poderá definir o endereço IP. Entre em contato com o administrador da rede para obter um endereço IP.
- O endereço IP pode estar sendo utilizado por outro dispositivo. Para verificar:
  1. Desconecte o dispositivo Axis da rede.
  2. Em uma janela de comando/DOS, digite `ping` e o endereço IP do dispositivo.
  3. Se receber: `Reply from <IP address>: bytes=32; time=10...` isso significa que o endereço IP já pode estar sendo usado por outro dispositivo na rede. Obtenha um novo endereço IP junto ao administrador da rede e reinstale o dispositivo.
  4. Se receber: `Request timed out`, isso significa que o endereço IP está disponível para uso com o dispositivo Axis. Verifique todo o cabeamento e reinstale o dispositivo.
- Pode haver um possível conflito de endereço IP com outro dispositivo na mesma sub-rede. O endereço IP estático no dispositivo Axis é usado antes que o DHCP defina um endereço dinâmico. Isso significa que, se o mesmo endereço IP estático padrão também for usado por outro dispositivo, poderá haver problemas para acessar o dispositivo.

Problemas com o acesso ao dispositivo

Não é possível fazer login ao acessar o dispositivo em um navegador

Quando o HTTPS estiver ativado, certifique-se de utilizar o protocolo correto (HTTP ou HTTPS) ao tentar fazer login. Talvez seja necessário digitar manualmente `http` ou `https` no campo de endereço do navegador.

Caso tenha perdido a senha da conta root, será necessário redefinir o dispositivo para as configurações padrão de fábrica. Para obter instruções, consulte *Restauração das configurações padrão de fábrica, on page 23*.

O endereço IP foi alterado pelo DHCP

Os endereços IP obtidos de um servidor DHCP são dinâmicos e podem mudar. Se o endereço IP tiver sido alterado use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede. Identifique o dispositivo usando seu modelo ou número de série ou nome de DNS (se um nome tiver sido configurado).

Se necessário, é possível atribuir um endereço IP estático de forma manual. Para obter instruções, vá para *axis.com/support*.

Erro de certificado ao usar IEEE 802.1X

Para que a autenticação funcione corretamente, as configurações de data e hora no dispositivo Axis deverão ser sincronizadas com um servidor NTP. Vá para **System > Date and time (Sistema > Data e hora)**.

O navegador não é compatível

Para obter uma lista dos navegadores recomendados, consulte *Suporte a navegadores, on page 5*.

Não é possível acessar o dispositivo externamente

Para acessar o dispositivo externamente, recomendamos que você use um dos seguintes aplicativos para Windows®:

- AXIS Camera Station Edge: grátis, ideal para sistemas pequenos com necessidades básicas de monitoramento.
- AXIS Camera Station Pro: versão de avaliação grátis por 90 dias, ideal para sistemas de pequeno a médio porte.

Para obter instruções e baixar o aplicativo, acesse *axis.com/vms*.

Problemas com MQTT

Não é possível conectar através da porta 8883 com MQTT sobre SSL.

O firewall bloqueia o tráfego que utiliza a porta 8883, uma vez que é considerado inseguro.

Em alguns casos, o servidor/broker pode não fornecer uma porta específica para a comunicação MQTT. Ainda será possível usar MQTT em uma porta normalmente usada para tráfego HTTP/HTTPS.

- Se o servidor/broker suporta WebSocket/WebSocket Secure (WS/WSS), geralmente na porta 443, use este protocolo em vez do MQTT. Verifique com o provedor do servidor/broker para saber se o WS/WSS é suportado e qual porta e caminho base devem ser usados.
- Se o servidor/corretor suportar ALPN, o uso do MQTT poderá ser negociado em uma porta aberta, como a 443. Verifique com seu provedor de servidor/corretor se há suporte para ALPN e qual protocolo e porta ALPN usar.

Se você não conseguir encontrar aqui o que está procurando, experimente a seção de solução de problemas em *axis.com/support*.

Considerações sobre desempenho

Ao configurar seu sistema, é importante considerar como diferentes configurações e situações afetam o desempenho. Alguns fatores afetam a largura de banda (taxa de bits), outros afetam a taxa de quadros e alguns afetam ambos.

Os fatores mais importantes a serem considerados são:

- Alta resolução de imagem ou níveis de compactação menores geram imagens com mais dados que, por sua vez, afetarão a largura de banda.
- O acesso por números elevados de clientes H.264/H.265/AV1 unicast ou clientes Motion JPEG pode afetar a largura de banda.
- A exibição simultânea de diferentes streams (resolução, compactação) por diferentes clientes afeta a taxa de quadros e a largura de banda.
  Use streams idênticos sempre que possível para manter uma alta taxa de quadros. Perfis de stream podem ser usados para garantir que streams sejam idênticos.
- O acesso a streams de vídeo com diferentes codecs afeta simultaneamente a taxa de quadros e a largura de banda. Para obter o desempenho ideal, use streams com o mesmo codec.
- O uso pesado de configurações de eventos afeta a carga da CPU do produto que, por sua vez, impacta a taxa de quadros.
- Usar HTTPS pode reduzir a taxa de quadros, especialmente se houver transmissão de Motion JPEG.
- A utilização pesada da rede devido à infraestrutura ruim afeta a largura de banda.
- A exibição em computadores clientes com desempenho ruim reduz o desempenho percebido e afeta a taxa de quadros.

- Executar vários aplicativos AXIS Camera Application Platform (ACAP) simultaneamente pode afetar a taxa de quadros e o desempenho geral.

Entre em contato com o suporte

Se precisar de ajuda adicional, acesse *axis.com/support*.

Cibersegurança

A segurança cibernética oferece suporte a um ciclo de vida de produto bem-sucedido com riscos minimizados. Você pode encontrar informações detalhadas e documentação sobre nossa abordagem à segurança cibernética em *axis.com/about-axis/cybersecurity*. Siga as diretrizes de segurança cibernética abaixo para receber notificações de segurança da Axis sobre o produto e para realizar a configuração do produto, de modo a garantir um ciclo de vida e um descomissionamento seguros.

No *Axis Trust Center*, você pode encontrar informações sobre como a Axis implementa a conformidade de segurança, a transparência, a proteção de dados e a privacidade.

Gerenciamento de vulnerabilidades

A Axis é uma *Autoridade de numeração de vulnerabilidades e exposições comuns (CVE) (CNA)*. Para minimizar seu risco de exposição, seguimos os padrões do setor ao identificar e resolver vulnerabilidades em nossos dispositivos, software e serviços. Consulte *axis.com/vulnerability-management* para obter informações sobre nossa política de gerenciamento de vulnerabilidades ou para relatar uma vulnerabilidade.

Notificações de segurança

Inscreva-se para receber emails de notificação de segurança da Axis em *axis.com/security-notification-service*. Enviaremos a você informações sobre vulnerabilidades, alertas de segurança correspondentes e outros assuntos relacionados à segurança do seu produto Axis.

Ciclo de vida seguro do produto

A Axis minimiza os riscos durante toda a vida útil de nossos produtos por meio do gerenciamento seguro do ciclo de vida. Use nossos guias para aumento do nível de proteção em *help.axis.com* para configurar e operar com mais segurança seus produtos Axis e para encontrar informações sobre:

Uso seguro desde o primeiro uso – Os produtos Axis são pré-configurados com alta proteção padrão para permitir a inicialização segura e a comunicação criptografada desde o início.

Uso pretendido e erros comuns de configuração – Nossos guias fornecem informações sobre o uso pretendido dos produtos Axis, incluindo erros comuns de configuração e usos indevidos relevantes para a segurança que devem ser evitados.

Gerenciamento de vulnerabilidades e transparência da cadeia de suprimentos – Uma lista de materiais de software (SBOM) é publicada com cada versão de software em *axis.com* para divulgar vulnerabilidades e aumentar a transparência da cadeia de suprimentos.

Descomissionamento e exclusão segura de dados – Para desativar um produto com segurança quando ele chegar ao fim de seu ciclo de vida, redefina-o para as configurações padrão de fábrica. Isso apaga suas configurações, dados armazenados e informações confidenciais.

Informações de segurança

Níveis de perigo

⚠ PERIGO

Indica uma situação perigosa que, se não evitada, irá resultar em morte ou lesões graves.

⚠ AVISO

Indica uma situação perigosa que, se não evitada, poderá resultar em morte ou lesões graves.

⚠ CUIDADO

Indica uma situação perigosa que, se não evitada, poderá resultar em lesões leves ou moderadas.

OBSERVAÇÃO

Indica uma situação perigosa que, se não evitada, poderá resultar em danos à propriedade.

Outros níveis de mensagens

Importante

Indica informações significativas que são essenciais para o produto funcionar corretamente.

Observação

Indica informações úteis que ajudam a obter o máximo do produto.

T10208511_pt

2026-10 (M19.2)

© 2024 – 2026 Axis Communications AB